RECEIVED
CENTRAL FAX CENTER

SEP 14 2006

REMARKS

Claims 1 – 11 are pending in this application.

In a Final Office Action mailed 07 June 2006, the Examiner rejected claims 1 – 11 under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Applicant has amended independent claims 1, 5 to provide additional specificity to traverse the Examiner's rejection of claim 1-11 under 35 USC §112, second paragraph.

The Examiner rejected claims 1, 2, 5, 8, 10, and 11 under 35 USC §102(b) as being anticipated by US Patent No. 6,049,612 issued to Fielder et al. and also rejected claims 3, 4, 6, and 7 under 35 USC §103(a) as being unpatentable over Fielder as applied to claims 1 and 5 above and further in view of U.S. Patent No. 6,381,695 issued to Kudo. The Examiner noted with respect thereto:

> As per claims 1, 5, 8 and 10:
> Fielder discloses a method for generating an encryption key comprising:
> retrieving the host identification from the host device for use as a private portion of an encryption key (4:29-31 wherein the E-Key Seed acts as the host identification (6:13-15) and is private since it is secret);
> generating at least one content variable that uniquely identifies a corresponding block of said file as a public portion of said encryption key (4:29-31 wherein the constant value is the content variable and is combined with the E-Key Seed to form the encryption key);
> combining the host identification and the at least one content variable to produce the encryption key that was used to encrypt the file (5:18-30);
> encrypting a block of plaintext data using the encryption key to produce a block of ciphertext (5:37-46);
> appending only the at least one content variable to the block of ciphertext (5:37-46);
> transmitting the block of ciphertext and the appended at least one content variable over the unsecured interface to the storage device (3:11-16);
> storing the block of ciphertext and the appended one or more content variables within the storage device (3:11-16); and
> decrypting the block of ciphertext with the encryption key to produce the block of plaintext (4:61-63).

Applicant has reviewed the cited Fielder Patent, the Examiner's clearly stated grounds of rejection and Applicant provides the following remarks in support of patentability of claims 1-11.

The present method for encryption key generation provides a method of combining the speed of conventional encryption with the security of public key encryption. The host device encrypting the plaintext to be transmitted over the unsecured interface is assigned a host identification. The host identification is stored in a secure location within the host device. The host

identification is analogous to the private key. Only the host device can generate the encryption key used to later decrypt the ciphertext. A second variable, a content identification, is generated by the host device. Each successive block of plaintext to be encrypted uses a different content identification. The host identification along with the content identification is used for generating an encryption key to encrypt a block of plaintext. This second variable, the content identification, is analogous to the public key. The content identification is transmitted with the resulting ciphertext and together the ciphertext and content identification are stored for retrieval at a later time. The encryption key is never transmitted with the file and is only stored in the host device to ensure that only the host device can decrypt the encrypted file. The encryption key is generated following a method that can be repeated later using the same host identification and content identification to generate the same encryption key. In other words, the formula used to generate the encryption key is deterministic.

This structure is recited in Applicant's independent claim 1 as follows:

> A method for generating an encryption key for use with a host device having a host identification stored therein, for encrypting a file which comprises a plurality of blocks of plaintext data in a manner that said encrypted file can only be decrypted by said host device, the method comprising:
>
> retrieving the host identification from the host device for use as a private portion of an encryption key;
>
> generating at least one content variable as a public portion of said encryption key, where said at least one content variable uniquely identifies a corresponding block of said file;
>
> combining the host identification and the at least one content variable to produce the encryption key;
>
> encrypting a block of plaintext data using the encryption key to produce a block of ciphertext;
>
> appending only the at least one content variable to the block of ciphertext; and
>
> storing the block of ciphertext and the appended one or more content variable within a storage device.

In contrast, the Fielder Patent discloses:

> A system for protecting sensitive information files and messages from access by unauthorized parties, whether stored in a computer memory or exchanged over a transfer medium between sending and receiving stations. Each document or message file is created in normal operation. A constant value or message is logically combined to a secret bit sequence (E-Key Seed) to perform a many-to-few bit mapping which shuffles the bits and provides a pseudo-random result. The result then is applied through a secure hash function generator to perform a second many-to-few bit mapping and provide a pseudo-random message digest. The message digest in turn may be truncated to a desired bit length to provide a deterministic but non-predictable, pseudo-random, symmetric encryption key which is used to encrypt the

> message or information file to be protected. The deterministic encryption key is destroyed immediately after use. The constant value and encrypted message thereupon are secure hashed to create a message integrity code (MIC) that is used to detect any alterations to the encrypted information file that may have occurred intentionally or unintentionally.

The Fiedler Patent fails to show or suggest creating an encryption key using data that is part public and part private where only the public portion of the data that is used to create the encryption key is transmitted with the coded file, such that only the host device that encrypted the file can decrypt the file because it is the only one that has the private portion of the data used to generate the encryption key. In particular, the Fiedler Patent discloses in column 6, lines 6-13:

> FIG. 6 shows the various bit fields that could make up a constant value 11. A length byte 50 indicates the total number of bytes in the constant value 11. The length byte is necessary because a number of the remaining bit fields of the constant value are of variable length. Following the length byte 50 is the E-Key Seed ID 51 which is used as a table look-up tag associated with the corresponding E-Key Seed stored in an E-Key Seed table.

Thus, the E-Key Seed ID 51 is part of the constant value and is transmitted to the recipient as part of the constant value 11. This contradicts the Examiner's assertion that:

> generating at least one content variable that uniquely identifies a corresponding block of said file as a public portion of said encryption key (4:29-31 wherein the constant value is the content variable and is combined with the E-Key Seed to form the encryption key);
>
> combining the host identification and the at least one content variable to produce the encryption key that was used to encrypt the file (5:18-30); (emphasis added)

It is clear from the diagram of Figures 3 and 4 that the E-Key Seed is combined with the constant value as two independent inputs to the hashing functions to generate the encryption key. In addition, Applicant recites that the private portion of the encryption key is NOT transmitted with the file: "appending only the at least one content variable to the block of ciphertext;" in contrast with the teaching of the Fiedler Patent where the E-Key Seed ID 51 is transmitted to the recipient as part of the constant value 11 so the recipient can look up the E-Key Seed from a shared lookup table. Furthermore, as shown in Figure 6 of the Fiedler Patent, the encryption algorithm is optionally transmitted to the recipient.

Applicant therefore believes that claims 1-2, 5, 8-11 are allowable under 35 USC §102(b) over the cited Fiedler Patent, since the Fiedler Patent teaches away from the specific elements recited in Applicant's independent claims 1 and 5.

The Examiner also rejected claims 3, 4, 6, and 7 under 35 USC §103(a) as being

unpatentable over Fielder as applied to claims 1 and 5 above and further in view of U.S. Patent No. 6,381,695 issued to Kudo. Applicant believes that claims 3, 4, 6, and 7 are allowable under 35 USC §103(a) over the cited Fiedler and Kudo Patents since these claims depend on allowable base claims. In addition, Kudo describes a third-party, key management agent as used in public key cryptography. In Kudo the third party (key management agent) is used to prevent party A from decrypting content outside of a time window as requested by a party B. Applicant's invention only involves party A trying to prevent any and all other parties from decrypting the content. The use of a time variable is not to give another party a finite window to decrypt the content, but instead to make it more difficult for any other party to attempt to derive the encryption key from the public content variable. Applicant's claims 3, 4, 6, and 7 recite the use of time in the creation of a public key component and not in a certificate or in the use of a fixed public key component. The time variable prevents a third party from 'cracking' a single content variable, that is being able to derive the decryption key from the content variable, because once the time variable changes the 'cracked' content variable is no longer valid since it would not correspond to the same encryption key. Applicant therefore believes that claims 3, 4, 6, and 7are allowable under 35 USC §103(a) over the cited references.

In summary, Applicant therefore believes that claims 1-11 are allowable under 35 USC §112, second paragraph, and under 35 USC §102(b) and 35 USC §103(a) over the cited references.

In view of the above amendments and remarks, Applicant believes the pending application is in condition for allowance. Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-1848, under Order No. 013208.0121PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: 14 September 2006

By: James M Graziano

James M. Graziano
Registration No.: 28,300
(303) 830-1776
(303) 894-9239 (Fax)
Attorney for Applicant

Customer No. 24283